REMARKS

Claims 1-33 remain in this application. No claims have been added, canceled, or amended.

INTERVIEW SUMMARY

The Examiner is thanked for the interview of March 16, 2004. In the interview, the Applicants' representative explained how Kumar failed to disclose the feature, "in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate," as recited in Claim 1 of the application. The Applicants' representative explained that Kumar's sending of a deliberately false response was indicative of a "zero" within a binary message, and not indicative of whether the sender of the false response was legitimate. The Examiner conceded that Kumar, by itself, did not disclose all of the limitations of Claim 1 as required by 35 U.S.C. 102.

CLAIM REJECTIONS – 35 U.S.C. § 102

The Office Action rejected Claims 1-6, 12-17, and 23-28 under 35 U.S.C. § 102(e) as allegedly unpatentable over Kumar et al., U.S. Patent No. 6,535,980 (Kumar). The rejection is respectfully traversed.

Independent Claim 1 recites a method for verifying the legitimacy of an untrusted mechanism. The method comprises:

> submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism;
> receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information;

determining whether each response received from the untrusted mechanism is a **correct response**; and
in response to a determination that **any** of the responses from the untrusted mechanism is an **incorrect response**, determining the untrusted mechanism to **not be legitimate**.

The method of Claim 1 is quite advantageous because it provides an effective means for testing the legitimacy of any untrusted mechanism. According to the method, an untrusted mechanism is determined to not be legitimate if any of the untrusted mechanism's responses to a sequence of information set submissions is an incorrect response. Because the sequence in which information sets are submitted to an untrusted mechanism is unpredictable to the untrusted mechanism, it is highly difficult, if not impossible, for an illegitimate untrusted mechanism to "fake" correct responses to all of the submissions.

Kumar does not teach or suggest such a method. Instead, Kumar discloses a technique for cryptographically and keylessly protecting a message by coding and transmitting the message as a binary string—all "ones" and "zeroes." Kumar discloses that a correct ("true") response to a receiver's challenge is sent in order to represent a "one" in a binary-coded message, and a deliberately incorrect ("false") response to a receiver's challenge is sent in order to represent a "zero" in the binary-coded message. In Kumar, the sending of a deliberately incorrect ("false") response to a challenge has no bearing whatsoever on the legitimacy of the mechanism that sent the deliberately incorrect response. Therefore, Kumar fails to teach or suggest at least Claim 1's limitation, "in response to a determination that **any** of the responses from the untrusted mechanism is an **incorrect response**, determining the untrusted mechanism to **not be legitimate**."

The Office Action hypothesizes that if the binary-coded message is a secret key, and one of Kumar's responses is a "false" response when it should have a "true" response, or vice-versa, then the secret key will contain erroneous bits, and information encrypted with the erroneous secret key will not be decryptable using an error-free version of the secret key. The Office Action then speculates that the inability of a first party to decrypt information that was allegedly encrypted by a second party using the same secret key could lead the first party to conclude that the second party is not legitimate—although Kumar contains no support or motivation for such speculation. In engaging in this speculation, the Office Action relies upon two different and inconsistent interpretations of what it means for a response to be "incorrect."

More specifically, in rejecting the limitation "in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate," the Office Action relies upon an interpretation of "incorrect response" that is inconsistent with the interpretation of "correct response" that the Office Action relies upon to reject another limitation of Claim 1, "determining whether each response received from the untrusted mechanism is a correct response."

Notably, the Office Action alleges that Kumar discloses Claim 1's limitation, "determining whether each response received from the untrusted mechanism is a correct response" at col. 4, lines 5-8. The text at col. 4, lines 5-8, refers to determining whether responses to challenges are "true" or deliberately "false." Therefore, in order to demonstrate that Kumar discloses this limitation, the Office Action analogizes Kumar's determination of whether a response is "true" to the claimed determination of whether a response is "correct." Thus, in order for Kumar to disclose this limitation, a "true"

response must be interpreted as a "correct" response, and a deliberately "false" response must be interpreted as an "incorrect" response.

It is inconsistent to mix this interpretation of Kumar with another, incompatible interpretation of Kumar that a response is "incorrect" if the response inadvertently causes a receiver to receive an erroneous bit of a binary-coded message, regardless of whether the response is a "true" or deliberately "false" response. If this latter interpretation of Kumar is used, then Kumar fails to disclose the limitation, "determining whether each response received from the untrusted mechanism is a correct response," because Kumar does not disclose determining anything about a response beyond whether the response is "true" or "false." No matter which interpretation of response correctness is used, Kumar fails to teach or suggest at least one limitation of Claim 1. For at least these reasons, Applicants submit that Claim 1 is patentable over Kumar.

Applicants further submit that Claims 2-6, which depend from Claim 1 and which recite further advantageous aspects of the invention, are also patentable over Kumar for at least the reasons given above in connection with Claim 1.

Claims 12-17 are apparatus claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 12-17 are patentable over Kumar for at least the reasons given above in connection with Claims 1-6, respectively.

Claims 23-28 are computer-readable medium claims, which are analogous to the methods of Claims 1-6, respectively. Applicants submit that Claims 23-28 are patentable over Kumar for at least the reasons given above in connection with Claims 1-6, respectively.

CLAIM REJECTIONS – 35 U.S.C. § 103

The Office Action rejected Claims 7-11, 18-22, and 29-33 under 35 U.S.C. § 103 as allegedly unpatentable over Kumar in view of Shostack et al., U.S. Patent No. 6,298,445 B1 (Shostack). The rejection is respectfully traversed.

Independent Claim 7 recites a method for verifying the legitimacy of an untrusted signature verification mechanism. The method comprises:

> submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being **known to be verifiable,** and said second signature being **known to be unverifiable**;
> receiving a response from the untrusted mechanism for each submission of either said first signature or said second signature;
> determining whether each response received from the untrusted mechanism is a **correct response**; and
> in response to a determination that **any** of the responses from the untrusted mechanism is an **incorrect response**, determining the untrusted mechanism to **not be legitimate**.

The method of Claim 7 provides an effective means for testing the legitimacy of an untrusted signature verification mechanism.

Kumar does not teach or suggest such a method. Kumar is discussed above with reference to Claim 1. As is discussed above, Kumar fails to teach or suggest at least the limitation, "in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate," which is also recited in Claim 7.

Shostack also fails to teach or suggest this limitation. In fact, the Office Action does not even allege that Shostack teaches or suggests this limitation. The Office Action relies upon Shostack only to disclose, allegedly, the use of digital signatures to authenticate the integrity of a software enhancement.

Additionally, Kumar fails to teach or suggest information (digital signature or otherwise) that is **known to be verifiable** and information that is **known to be unverifiable**. The Office Action relies on Kumar's col. 3, lines 40-55, to allegedly disclose information that is known to be verifiable and information that is known to be unverifiable. However, this text merely discusses authentication schemes. The cited text says nothing about information that is known to be verifiable or unverifiable. Therefore, Kumar, taken individually, fails to teach or suggest Claim 7's limitation, "submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said **first signature being known to be verifiable, and said second signature being known to be unverifiable**."

Shostack also fails to teach or suggest this limitation. In fact, the Office Action does not even allege that Shostack teaches or suggests this limitation. The Office Action relies upon Shostack only to disclose, allegedly, the use of digital signatures to authenticate the integrity of a software enhancement. The Office Action does not even allege that Shostack discloses or suggests digital signatures that are known to be verifiable or unverifiable.

Even combined (assuming arguendo that it would have been obvious to combine the references), Kumar and Shostack fail to teach or suggest all of the limitations of Claim 7. As discussed above, neither of these references discloses or suggests "in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate." Also as discussed above, neither of these references discloses or suggests, "submitting a first signature and a second signature to an untrusted signature verification mechanism in a sequence that is unpredictable to the untrusted mechanism, said first signature being

known to be verifiable, and said second signature being known to be unverifiable." Thus, even if the references were combined, they would still fail to disclose or suggest these aspects of Claim 7. For at least these reasons, Applicants submit that Claim 7 is patentable over Kumar and Shostack, taken individually or in combination.

Applicants further submit that Claims 8-11, which depend from Claim 7 and which recite further advantageous aspects of the invention, are also patentable over Kumar and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claim 7.

Claims 18-22 are apparatus claims, which are analogous to the methods of Claims 7-11, respectively. Applicants submit that Claims 18-22 are patentable over Kumar and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claims 7-11, respectively.

Claims 29-33 are computer-readable medium claims, which are analogous to the methods of Claims 7-11, respectively. Applicants submit that Claims 29-33 are patentable over Kumar and Shostack, taken individually or in combination, for at least the reasons given above in connection with Claims 7-11, respectively.

For at least the reasons set forth above, Applicants respectfully submit that all pending claims are patentable over the art of record, including the art cited but not applied. Accordingly, allowance of all pending claims is respectfully solicited.

The Examiner is invited to telephone the undersigned at (408) 414-1080 to discuss any issue that may advance prosecution.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: March 17, 2004

Christian A. Nicholes
Reg. No. 50,266

1600 Willow Street
San Jose, California 95125-5106
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Non Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on 3/17/04 by